Wukill, Manfaatkan Celah Lama Windows

Anda mungkin baru mendengar nama virus yang satu ini. Tapi, itu bukan berarti virus ini tidak "terkenal" seperti layaknya Brontok. Virus ini hampir selalu berhasil menduduki peringkat 10 besar Asia dalam tingkat penyebarannya. Penasaran *kan*?

Arief Prabowo

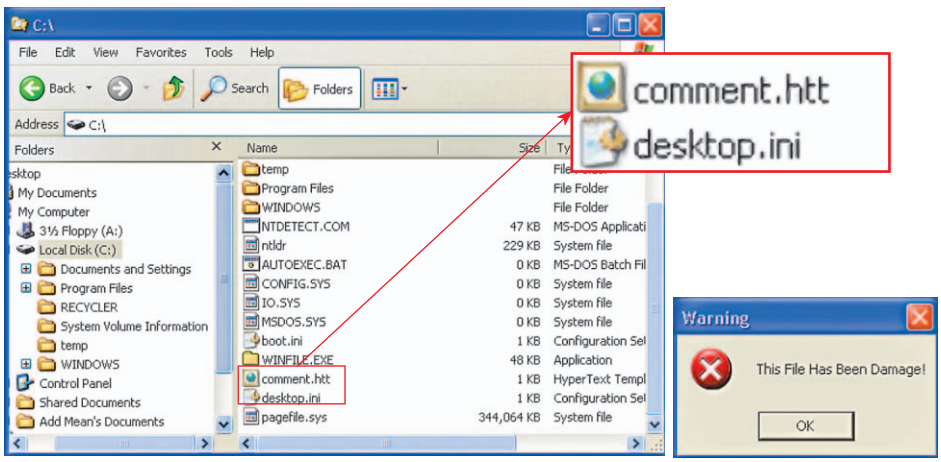
Virus lama belum tentu kalah dengan virus baru. Wukill contohnya, virus yang dikenal juga dengan nama Rays ini, pada salah satu situs yang menyediakan informasi statistik penyebaran virus di seluruh dunia, Wukill hampir selalu mendapatkan peringkat 10 besar di wilayah Asia, bahkan terkadang bisa masuk peringkat tiga besar. Tapi tentunya, ini masih di bawah Brontok yang hampir rata-rata selalu menjadi peringkat pertama dalam tingkat penyebaran virus di Asia, bahkan terkadang masuk tiga besar dunia.

Menurut pantauan kami, Wukill yang berasal dari negeri China ini memang sudah banyak menyebar luas di masyarakat. Virus ini diprogram menggunakan bahasa Visual Basic 6.0, tanpa di-*compress* ataupun dienkripsi. Pada sampel yang kami punya, virus ini memiliki ukuran file sebesar 49.152 bytes.

Penampilan

Virus ini menggunakan icon folder sebagai icon utama dari program virus. Anda semua pasti sudah tahu maksudnya. Ya, *social engineering* yang digunakan untuk mengelabui sang *user*. Ini juga yang dilakukan oleh virus-virus baru, khusunya virus lokal yang sekarang ini sedang gencar-gencarnya bermunculan, yang rata-rata menggunakan icon folder sebagai kamuflase. Namun, apabila Wukill berjalan pada *operating system* selain Windows 9x, Windows XP misalnya, jika dilihat secara saksama maka akan terlihat perbedaan antara icon folder yang dimiliki virus dengan icon folder yang asli. Tentunya ini akan membuat si user curiga.

Apabila Anda mengeksekusi virus ini, ia akan menampilkan *error message* yang menyatakan kalau file yang Anda eksekusi tersebut rusak atau *damage*. Sebenarnya ini hanya "akal-akalan" sang virus, karena sebetulnya ia sudah menetap di memory.



File desktop.ini dan comment.htt yang digunakan untuk mengeksploitasi celah Windows.

Error warning palsu dari Wukill.

Teknik Penyebaran

Wukill akan memeriksa apakah disket pada drive A: dapat diakses, kalau ya maka virus akan segera meng-*copy*-kan dirinya sendiri ke disket tersebut menggunakan nama Winfile.exe. Tidak hanya itu, virus juga akan mencoba untuk meng-copy-kan dirinya ke setiap drive harddisk, flashdisk, ataupun media penyimpan data lainnya. Wukill juga dapat menyebar melalui *sharing* folder dan e-mail.

Pada saat aktif di memory, virus ini akan selalu memonitor kegiatan Anda pada Windows Explorer dan biasanya akan meng-copy-kan dirinya pada direktori yang sedang aktif. Pada sampel virus Wukill yang kami punya, ia juga akan membuat dua buah file tambahan, yakni berupa file dengan nama 'desktop.ini' dan 'comment.htt' dengan attribut *hidden* dan *system*. File tersebut berguna apabila sang user membuka sebuah folder yang di-share pada komputer *remote*, maka dengan otomatis virus akan meng-copy-kan dirinya sendiri ke komputer tersebut.

Ini bisa dilakukan sang virus karena ia telah mengeksploitasi celah dari Microsoft VM ActiveX Component dengan menggunakan file comment.htt yang dibuatnya tadi. Inilah mengapa sebabnya virus ini baru dapat berjalan optimal pada Windows 9x, karena pada Windows yang lebih baru, celah tersebut sudah diperbaiki oleh Microsoft. Namun, hal tersebut tidak membuat virus ini berkecil hati karena buktinya ia masih dapat menyebar dengan luas. Pada beberapa antivirus, file comment.htt ini juga terdeteksi sebagai virus VBS.Starter.

Seperti yang tadi dikatakan, bahwa Wukill juga akan menyebarkan dirinya melalui e-mail. Virus akan membaca semua e-mail address yang ada pada Address Book Microsoft Outlook, lalu mengirimkan dirinya ke e-mail tersebut. Anda harus berhati-hati apabila me-

Tabel perubahan registry yang dilakukan oleh Wukill.

Registry	Nilai	Tujuan
HKEY_LOCAL_MACHINE \\SOFTWARE\Microsoft\Windows \CurrentVersion\Run\RavTimeXP	%Windows% \MsTray.exe dan random.	Penambahan value pada section run agar virus dapat berjalan otomatis pada saat start windows.
HKEY_CURRENT_USER\Software \Microsoft\Windows\CurrentVersion \Explorer\CabinetState	1 (dword)	Agar pada title bar dari Windows Explorer menampilkan Full Path dari direktori aktif.
HKCU\Software\Microsoft \Windows\CurrentVersion \Explorer\Advanced\HideFileExt	1 (dword)	Selalu menyembunyikan ekstension dari file.
HKCU\Software\Microsoft \Windows\CurrentVersion \Explorer\Advanced\Hidden	0 (dword)	Sembunyikan file dengan attribut hidden.

nerima e-mail dengan *attachment* 'MShelp. EXE', karena siapa tahu Anda sedang dikirimi virus Wukill.

Bagaimana Ia Menginfeksi?

Pada saat kali pertama virus dieksekusi, ia akan membuat sebuah file induk yang ditanam pada direktori Windows dengan nama MsTray. exe. Lalu, ia akan membuat file tersebut agar otomatis dieksekusi pada saat start Windows dengan melakukan perubahan pada registry, yaitu pada key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, dengan name value RavTimeXP, maka virus akan selalu aktif di memory.

Tak hanya itu, Wukill juga melakukan beberapa perubahan lagi pada registry untuk memperlemah sistem dari Windows, agar virus dapat dengan lancar menginfeksi komputer tersebut. Sepertinya virus ini masih berbaik hati, karena Task Manager, Regedit, ataupun MsConfig masih bisa kita akses, karena tidak diblok oleh sang virus.

Cerdik dan Jahil

Satu hal yang sangat menarik dari virus ini adalah file induknya akan selalu berubah-ubah. Contohnya apabila pada saat start windows, virus dijalankan dari C:\Windows\MsTray.exe. Lalu saat sang user melakukan eksplorasi dengan Windows Explorer ke direktori C:\Windows, otomatis pada *title bar* akan berisi "C:\Windows", maka dari sini virus mengetahui bahwa direktori tempat file induk virus tersebut sama dengan direktori yang sedang dieksplorasi oleh user.

Selanjutnya untuk menghindari dari "kejaran" sang user, virus akan menghapus dirinya pada direktori tersebut, lalu membuat file induk lagi dengan nama dan direktori *random* yang biasanya ia ciptakan pada subdirektori system, web, fonts, temp, help, atau pada root direktori Windows. Lalu dari sini ia akan mengubah *registry run value* yang telah ia buat sebelumnya agar mengarahkan kepada nama file induk yang baru.

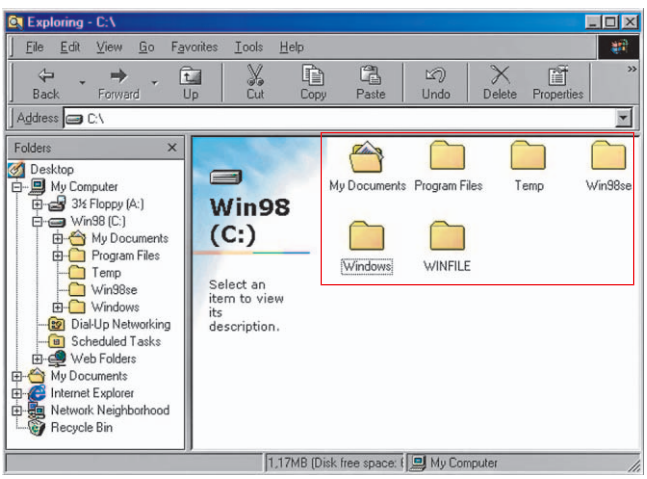
Disinilah terbukti betapa bergunanya perubahan registry untuk selalu menampilkan full path pada title bar Windows Explorer bagi sang virus.

Tak hanya cerdik, virus ini pun sedikit jahil, yakni akan terus menerus mengcopy-kan string "Hello!" ke clipboard Windows. Akibatnya, setiap kali kita akan melakukan paste terhadap string yang kita copy, yang muncul bukan string yang di-copy-kan, tapi string yang dibuat oleh sang virus yakni 'Hello!'.

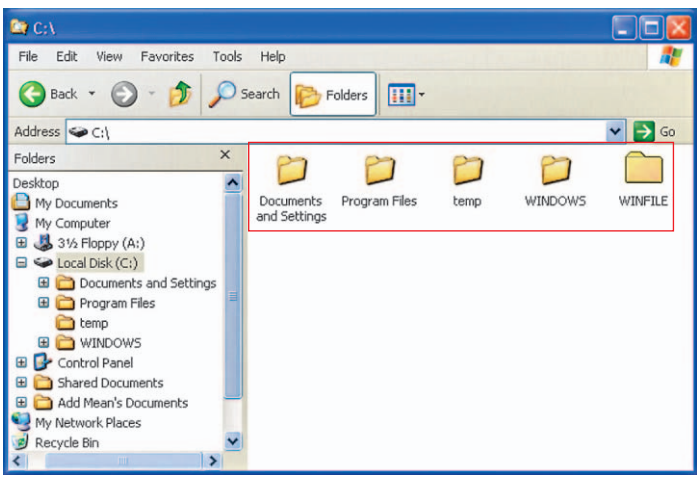
Membasmi Wukill

Pembasmian virus Wukill secara manual sepertinya masih bisa dilakukan. Karena virus ini dibuat menggunakan Visual Basic 6.0, kita bisa saja membuat virus ini crash, yakni dengan cara me-rename sementara file Visual Basic Run Time Library, yang biasanya terdapat dalam folder system Windows dengan nama MSVBVM60.DLL. Hanya saja tidak hanya virusnya yang mati, tapi semua program yang dibuat menggunakan bahasa Visual Basic 6.0 tidak akan dapat berjalan. Tapi sebenarnya, Anda tidak perlu repot karena kami tim PC Media Antivirus telah meng-update database dari PC Media Antivirus, agar dapat mengenali dan membasmi virus ini secara tuntas dan akurat hingga 100%.

PCMAV RC3 edisi lalu, pada beberapa komputer tidak dapat berjalan dengan sempurna, ini bisa diakibatkan karena terjadi bentrok dengan program lain yang sedang *running*, misalnya *real-time-protection* dari antivirus lain. Untuk itu, pada RC4 kali ini kami telah memperbaikinya agar dapat berjalan dengan baik. ■



Icon folder yang tampak sama jika dilihat dari Windows 98.



Icon folder yang tampak beda jika dilihat dari Windows XP.